AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: BH 5-14-2024

amg 5/15/24

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION WITHIN THE GOOGLE DRIVE ACCOUNT(s) ASSOCIATED WITH THE GOOGLE ACCOUNTS **rim.tarhuni@gmail.com** and **meltarhoni@gmail.com** THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. M-24-437-AMG

FILED
MAY 15 2024
JOAN KANE, CLERK
U.S. DIST. COURT, WESTERN DIST. OKL.
BY _____, DEPUTY

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following [Person or Property?] :

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B)	Possession/Accessing Child Pornography
18 U.S.C. § 2252A(a)(1)	Transportation of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Andrea Salazar, Homeland Security, which is incorporated by reference herein.

- ☐ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Andrea Salazar
Applicant's signature

Andrea Salazar
Special Agent
Homeland Security

Sworn to before me and signed in my presence.

Date: 5/15/24

Judge's signature

City and State: Oklahoma City, Oklahoma

AMANDA MAXFIELD GREEN, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION WITHIN THE GOOGLE DRIVE ACCOUNT(s) ASSOCIATED WITH THE GOOGLE ACCOUNTS **rim.tarhuni@gmail.com** and **meltarhoni@gmail.com** THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Andrea Salazar, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Google Drive accounts that are stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am currently employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so since July 2022. Prior, I was a federal police officer with Pentagon Force Protection Agency and had been so employed since August 2019. I hold a bachelor's degree in criminology and a Master of Public Administration from St. Mary's University. I also hold a Master of Science in Criminal Justice from Sam Houston State University. I am currently assigned to HSI Office of the Resident Agent in Charge Oklahoma City, Oklahoma. As part of my various duties and responsibilities, I investigate federal criminal cybercrime violations. As it relates to cybercrime, I have gained experience conducting child exploitation and child pornography investigations. My working experience has been augmented by training I received at the Federal Law Enforcement Training Center. Moreover, I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators. I have become aware of numerous examples of child pornography. Additionally, I have had the opportunity to observe and review hundreds of images and videos of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252 and 2252A, and I am authorized by law to request a search warrant. I have personally participated in the investigation described herein and have witnessed some of the facts and circumstances

described herein. The information set forth in this affidavit is based on my own observations and review of documents, or reliable information provided to me by other law enforcement personnel. I believe that there is probable cause to believe that evidence of possession/accessing and transportation of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(1), respectively, will be found in Google Drive accounts associated with the Google accounts **rim.tarhuni@gmail.com** and **meltarhoni@gmail.com** ("the TARGET ACCOUNT(s)"). Because this affidavit is being prepared for the limited purpose of securing the requested search warrant, I have not set forth all facts known to me about this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of the foregoing offenses, as further described in Attachment B, will be found in the TARGET ACCOUNT(s), as further described in Attachment A.

JURISDICTION

3. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

4. On January 23, 2024, HSI Oklahoma City received information from the Oklahoma State Bureau of Investigations (OSBI) regarding a Cyber Tip Line Report 184951099 from the National Center For Missing and Exploited Children (NCMEC). The

electronic service provider (ESP) Google LLC reported content containing child exploitation material in a Google Drive infrastructure. The suspect's email address is rim.tarhuni@gmail.com and/or meltarhoni@gmail.com, screen/user name is Rim Tarhuni, with a mobile phone number +14053321326 (verified 06/07/2020 21:28:32 UTC). The IP address provided on the report was 70.174.239.47. The Cyber Tip Report 184951099 reported the ISP as Cox Communications.

5. On January 26, 2024, HSI Oklahoma City received information from the OSBI regarding an additional Cyber Tip Line Report 185070213 from NCMEC. The ESP Google LLC reported content containing child exploitation material in a Google Drive infrastructure. The suspect's email address is rim.tarhuni@gmail.com and/or meltarhoni@gmail.com, screen/user name is Rim Tarhuni, with a mobile phone number +140533211326 (verified 06/07/2020 21:28:32 UTC). The IP address provided on the report was 70.174.239.47. The Cyber Tip Report 184951099 reported the ISP as Cox Communications.

6. On February 1, 2024, I submitted a subpoena to Cox Communications for data related to IP address 70.174.239.47. The response was provided on February 15, 2023. The account related to the IP address was registered to a **Maher ELTARHONI** (the SUBJECT INDIVIDUAL). The subscriber information for the account was Maher ELTARHONI, at 7500 NW 149th Cir, Oklahoma City, OK 73142-7805 (i.e., the SUBJECT PREMISES). The telephone number listed for the subscriber information was

405-332-1326 and an email address of maher.eltarhoni@okstate.edu. The account start date is listed as July 3, 2019.

7. On February 6, 2024, through the utilization of a law enforcement database, it was determined that the SUBJECT INDIVIDUAL entered the United States on July 15, 2009, through the issuance of an F-1 visa, an academic status to enter the United States. the SUBJECT INDIVIDUAL is originally from Libya. the SUBJECT INDIVIDUAL married Cristina Garcia on July 9, 2012. On January 23, 2013, Cristina Garcia petitioned for the SUBJECT INDIVIDUAL to become a United States Citizen. January 14, 2015, the SUBJECT INDIVIDUAL was approved for an I-485, an application to Register Permanent Residence or Adjust Status, and became a naturalize citizen on July 12, 2017. the SUBJECT INDIVIDUAL divorced Cristina Garcia on January 31, 2018. the SUBJECT INDIVIDUAL then married Dang Hong Tran Ngoc on October 7, 2018.

8. On February 7, 2024, through the utilization of a law enforcement database, it was determined that the SUBJECT INDIVIDUAL has a 2021 Nissan Rogue, Oklahoma license plate NHE120, registered in his name.

9. On February 15, 2024, after receiving the information from Cox Communications, I checked the Oklahoma County Assessor's Office public records and discovered the deed to the subject's premises was granted to the SUBJECT INDIVIDUAL and Dang Hong Tran Ngoc on December 20, 2023.

10. On February 20, 2024, Google Legal Investigations Support confirmed the formal request for the preservation of records and other evidence pursuant to 18 U.S.C.

2703(f) pending further legal process for the SUBJECT INDIVIDUAL's Google accounts rim.tarhuni@gmail.com and meltarhoni@gmail.com (the TARGET ACCOUNT(s)).

11. On March 21, 2024, I reviewed the material received by NCMEC. Previously mentioned Cyber Tip 184951099: Google LLC. reported that 15 files were uploaded to the suspect's Google Drive account associated with **rim.tarhuni@gmail.com** and **meltarhoni@gmail.com** on January 19, 2024, at 12:20:05 UTC. I reviewed three of the files. One file showed a video depicting a pubescent female showing her vagina. Another video showed three pubescent children, one female and two males engaging in sexual intercourse and exposing of genitalia area. A third file that was uploaded showed a video of two prepubescent females showering together and exposing their vagina.

12. Previously mentioned Cyber Tip 185070213: Google LLC. reported that two files were uploaded to the suspect's Google Drive account associated with **rim.tarhuni@gmail.com** and **meltarhoni@gmail.com** on January 19, 2024, at 04:18:03 UTC. I reviewed the files. One file showed three prepubescent minors, one female and two males, engaging in sexual intercourse and exposing of genitalia area. The second file depicted two prepubescent females completely naked, exposing their vaginas and engaged in sexually explicit conduct.

13. On April 11, 2024, United States Postal Inspection Service (USPIS) confirmed that The Hefner Station letter carrier stated he delivers mail to the SUBJECT

INDIVIDUAL at: the SUBJECT PREMISES (7500 NW 149th Cir OKC 73142). The Yukon Post Office stated there is a forwarding order from 11616 SW 7th St to the SUBJECT PREMISES, effective January 1, 2024, in the name of Maher Eltarhoni and Elta Design Company.

14. On May 9, 2024, Homeland Security Investigations executed a federal residential warrant at the SUBJECT PREMISES. At the time of execution, a male subject was encountered inside the residence and later identified as Fares Saleh Tarhuni. Fares. He stated that the residence belonged to his brother, the SUBJECT INDIVIDUAL, and his wife. Fares also stated that the SUBJECT INDIVIDUAL, his wife, and their two-year-old daughter live at the residence as well but left on the evening of May 8, 2024, to Colorado for a family vacation. Fares Tarhuni stated that his brother will be returning to Oklahoma City via Southwest airlines through Will Rogers Airport on May 11, 2024. Fares Tarhuni stated his brother (the SUBJECT INDIVIDUAL) has an iPhone in his possession.

15. On May 11, 2024, Homeland Security Investigations executed a federal search warrant on the SUBJECT INDIVIDUAL at Will Rogers World Airport, 7100 Terminal Dr, Oklahoma City, OK 73159. An iPhone and laptop were seized pursuant by the warrant from the SUBJECT INDIVIDUAL's person.

16. The SUBJECT INDIVIDUAL agreed to speak to Special Agent (SA) Joshua Dickson and myself. The SUBJECT INDIVIDUAL was advised of his rights per *Miranda*, and he provided verbal acknowledgment that he understood his rights. The SUBJECT

INDIVIDUAL provided the agents with his date of birth, March 1, 1991. He stated his cell phone number was 405-332-1326. The email addresses he provided during the interview were meltarhoni@gmail.com and maher.e@eltadesigngroup.com. The phone number and the Google email address ELTARHONI provided match the suspect's email address and phone number from the original NCMEC CyberTip. ELTARHONI also confirmed during his interview that his internet provider was Cox Communications.

BACKGROUND CONCERNING GOOGLE[1]

17. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

18. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops,

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

19. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

20. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

21. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

22. Google also offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and

automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely unless the user deletes them.

23. Additionally, Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

24. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts

created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

25. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

26. Google also provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

27. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

28. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet

must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

29. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

30. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. The subscriber information, saved photos, documents, messages, and emails associated with the TARGET ACCOUNT(s) will help establish who owns the TARGET ACCOUNT(s) and determine who uploaded child pornography images in the social media accounts associated with the TARGET ACCOUNT(s) listed in the NCMEC CyberTip reports.

31. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. For example, images of child pornography

may be stored within the Google Photos service associated with the TARGET ACCOUNT(s). Further, data from the TARGET ACCOUNT(s)' Chrome history, "My Activity" feature, and messaging services could provide evidence of the suspect's acquisition and subsequent distribution of child pornography.

32. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

33. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

34. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of downloading and possessing child pornography. In addition, emails, instant messages, Internet activity, and documents can lead to the identification of other instrumentalities of the crimes under investigation.

35. Therefore, Google's servers are likely to contain stored electronic communications and information concerning the subscriber of the TARGET ACCOUNT(s) and his or her use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

36. Based on the foregoing, I request that the Court issue the proposed search warrant.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Andrea Salazar
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on May 15th, 2024.

AMANDA MAXFIELD GREEN
United States Magistrate Judge
Western District of Oklahoma

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Google Drive account(s) associated with Google accounts **rim.tarhuni@gmail.com** and **meltarhoni@gmail.com** ("TARGET ACCOUNT(s)") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose to the government for the TARGET ACCOUNT(s) listed in Attachment A the following information, from January 1, 2024, to the present, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the TARGET ACCOUNT(s), including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the TARGET ACCOUNT(s), including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the TARGET ACCOUNT(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;

d. The contents of all media associated with the TARGET ACCOUNT(s) in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; all associated logs of each record, including the creation and change history, access logs, and IP addresses; and any settings that may indicate that images or other data were automatically uploaded from the synced device to Google Photos;

e. The contents of all records associated with the TARGET ACCOUNT(s) in Google Drive (including Docs, Sheets, Forms, and Slides), including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

f. The contents of all text, audio, and video messages associated with the TARGET ACCOUNT(s), including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the

size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government.

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(1), possession/accessing and transportation of child pornography, respectively, related to the dates of January 1, 2024, through the present, including, for the TARGET ACCOUNT(s) listed on Attachment A, information pertaining to the following matters:

a. Evidence of the possession, access with intent to view, and transportation of images depicting children engaged in sexually explicit conduct;

b. Evidence indicating how and when the TARGET ACCOUNT(s) was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the TARGET ACCOUNT(s) owner's state of mind as it relates to the crimes under investigation;

d. The identity of the person(s) who created or used the TARGET ACCOUNT(s), including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents,

attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Affiant may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.